

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS		X		
5	DDI				
6	DDA		X		
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO				
20					
21					
22					
SUSPENSE		Date			

Remarks

STAT

Executive Secretary

FOR 9 Mar 85
Date

3637 (10-81)

NTISSC

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY
COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

Comm

NTISSC 10-85
4 March 1985

11 MAR 1985

MEMORANDUM FOR THE MEMBERS AND OBSERVERS, NATIONAL
TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

SUBJECT: Minutes of the 15 February 1985 Meeting of the NTISSC

LOGGED

This memorandum forwards the minutes of the second meeting of the NTISSC, held on 15 February 1985. If no written corrections or changes to these minutes are received by 22 March 1985, they will stand as written.

STAT



Atch:
Meeting Minutes w/l Enclosure

~~FOR OFFICIAL USE ONLY~~

MINUTES OF THE 15 FEBRUARY 1985 MEETING
OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION
SYSTEMS SECURITY COMMITTEE (NTISSC)

1. The second meeting of the NTISSC was held on Friday, 15 February 1985, at the Federal Aviation Administration (FAA) building. With the exception of the NSC representative, all other agency and department representatives and observers were present.

2. The Chairman opened the meeting with an expression of appreciation to the Transportation representative for hosting the Committee meeting, after which the Transportation representative welcomed the Committee to the FAA facility.

3. NTISSC's meeting schedule for the remainder of 1985 was provided by the Chairman. The NTISSC will meet again on 10 May, 9 August and 8 November 1985, from 0900 to 1100 hours. Notification of meeting location(s) will be forwarded with each meeting agenda.

4. Two items on the subject of membership were next addressed:

a. The Chairman announced that the U.S. Nuclear Regulatory Commission (NRC) had joined the NTISSC in an observer status and introduced NRC's representative, Mr. Raymond J. Brady.

b. The second item regarding membership was Mr. William J. Casey's request to Secretary Weinberger for the Director of Central Intelligence (DCI) to have two representatives on the NTISSC and its subcommittees. The Chairman stated that the Central Intelligence Agency is currently represented on the Committee, and it was Mr. Casey's request that the Intelligence Community (IC) Staff also be represented. The Chairman went on to say that in the NTISSC Governing Procedures there existed a provision for this request, and the subject was then opened for discussion and comment.

The NSA representative stated he had no objection to the IC Staff initially participating in the NTISSC as an observer, and the JCS representative agreed. The DIA and CIA representatives were asked to provide comments and both agreed with the suggestion. The Chairman concluded the discussion on this subject by stating that without objection he would recommend that the IC Staff provide a representative to the NTISSC to participate initially as an observer.

5. The Executive Secretary reviewed current issues before the Committee for comment and vote. Particular mention was made of the KGV-10/TSEC release request, specifically the tardiness of some vote responses. At this point, some of the representatives expressed concern at not having received the correspondence. The importance of timely responses was stressed, especially in cases of equipment release requests. The Executive Secretary further stated he anticipated another six issues requiring comments, and one issue requiring a vote response to be forwarded to the Committee representatives in the near future. These issues, listed below, will have a 30-day response requirement.

Directive on NTISS Issuance System
COMSEC Classification Instruction
DES Instruction
AUTOSEVOCOM Doctrine Instruction
COMSEC Equipment Instruction
KW-46 Fleet Broadcast Instruction, and
TSEC/KG-30 release request (for vote).

6. The next subject discussed by the Committee was the National Policy on Application of Communications Security to Civil (U.S. Government and Commercial) Space Systems. Formal vote on this policy was delayed from the 8 November 1984 meeting due to concern that the private sector had not been fully informed. The FCC and NCS representatives provided feedback from the private sector; the findings of both representatives was that while the private sector does not disagree on the need to provide satellite security, there still exists a need for more definition and clarification of the policy. (The staff paper prepared by FCC which summarizes the questions and issues raised at the NIAC Communications Common Carrier Subcommittee meeting on 29 January 1985, is enclosed. Copies of the vugraphs used in the briefing presented by the NCS representative are available upon request from the NTISSC Secretariat.)

Discussion followed as to how the Committee would best resolve the questions and concerns put forth by the private sector. The idea of forming a working group was viewed as being too time-consuming and unproductive. The Commerce representative suggested another approach to the private sector via letter. It was further suggested by the NCS representative that NSA undertake the necessary revision of the policy, to which NSA agreed. The Chairman stated that this issue would be brought up again for vote at the 10 May NTISSC meeting.

The question of funding surfaced throughout the discussion of this policy; the Chairman emphasized that funding would not be provided by the Federal Government.

7. A briefing was presented by the Chairman of the Subcommittee on Telecommunications Security (STS) on The Evaluation of the Security Status of National Telecommunications. The STS Chairman stated that the report was still in a draft status and was the result of the Subcommittee's meeting on 12 February. He expected to provide a finalized version of this report by 25 February. He said that the report was approved by the Subcommittee representatives, with an abstention by CIA and a non-concurrence by OMB.

The briefing consisted of a summary of the STS report (copies of this report were provided to the Committee representatives prior to the meeting). The STS Chairman stated that as of today our communications are still very vulnerable. During the briefing the NTISSC Chairman questioned use of the phrase "NO ACCEPTED DEFINITION OF A GOVERNMENT-WIDE COMMUNICATIONS NETWORK", and the STS Chairman agreed to rephrase that term. (Copies of the vugraphs used in the STS briefing are available upon request from the NTISSC Secretariat.)

8. A briefing was also presented by the Chairman of the Subcommittee on Automated Information Systems Security (SAISS) on The First Annual Evaluation of the Status of Automated Information Systems Security (AISS) in the U.S. Government. The SAISS Chairman stated that this was the Subcommittee's final report, which had been formally approved on 7 February. With the exception of one abstention by NCS (because they had not received the report) and one non-concurrence by OMB, all other Subcommittee representatives concurred on the report.

This briefing also consisted of a summary of the SAISS report (copies of this report were provided to all Committee representatives prior to the meeting). In essence the report stated that the status of automated information systems security was poor and declining.

The SAISS Chairman also included the subject of the interaction between the SAISS and the STS, upon which the NTISSC Chairman remarked that the two Subcommittees appeared to be working well together. (Copies of the vugraphs used in the SAISS briefing are available upon request from the NTISSC Secretariat.)

At the conclusion of the SAISS briefing, the Chairman stated that no further revisions were planned for these reports. As soon as the final STS report was received the two reports would be merged and published during the March timeframe.

9. In the discussion that followed the briefings presented by the two Subcommittee Chairmen, the JCS representative commented that the greatest problem was the volume of information

being moved from one agency to another, and he felt that it was volume which needed to be considered on both sides of the assessment. There was much discussion regarding the securing of communications. In particular, the NTISSC expressed concern that the new upgrade of the FTS would not contain all the necessary security requirements. The GSA representative stated that every attempt had been made to incorporate these security requirements into the GSA upgrade, but that cost was a major consideration. She requested advice and assistance from the Subcommittee Chairmen on how these requirements might best be met, and the STS Chairman responded with an offer to assist.

STAT 10. The NSA representative provided a briefer, [redacted], to present the NSA views of how the telecommunications systems security programming and budget process/system would work. Only a portion of the actual briefing had been presented when the Committee representatives began to discuss the budget process and related problems.

Many present agreed that the existing budgeting process was inconsistent. The FEMA representative commented that it was difficult to project a five year plan, when in fact, OMB had only approved funding every other year.

The NSA representative questioned the OMB representative as to whether or not OMB was going to be able to bring the budgeting together for COMSEC for the total Government. The OMB representative's response was that he believed it would be centralized, and stated that what OMB was requesting, was for the data from all agencies and departments to be collected (in terms of resources required to fix the critical areas), provide a set list of those areas to be fixed, and submit a request through the Steering Group and the National Manager.

11. The Chairman closed the meeting by saying he looked forward to the next meeting of the NTISSC in May.

1 Enclosure

NATIONAL TELECOMMUNICATIONS AND INFORMATION

SYSTEMS SECURITY COMMITTEE

February 15, 1985

Handout by Managing Director,
Federal Communications Commission

1. FCC Staff Paper
2. Minutes of NIAC Meeting

February 7, 1985

NATIONAL POLICY ON APPLICATION OF COMMUNICATIONS
SECURITY TO COMMERCIAL SATELLITE TELEMETRY,
TRACKING AND CONTROL (TT&C)

1. Purpose

This paper summarizes issues raised at the NIAC Communications Common Carrier Sub-Committee meeting on January 29, 1985 and incorporates additional information obtained from discussions with sub-committee members and FCC staff after the meeting.

2. Need for Protection of TT&C

a. There was no disagreement at the NIAC meeting on the need to provide some measure of security for TT&C. Carriers contend that they already provide some security measures. Further they suggested several options to the government recommended technique for provision of TT&C security which they believe may be much less costly and equally effective in countering the threat. Options suggested include: (1) continuous high powered uplink; (2) an increase in command power threshold after satellite orbit is established; (3) shaped TT&C antenna beam to reduce the probability of disruption from offshore points; and (4) intrusion detection to permit immediate activation of countermeasures.

b. While carriers apparently concur in the government's objectives in this matter, they have serious concerns and numerous unanswered questions regarding: the application of the proposed national policy statement; what techniques might be approved by the government for providing secure TT&C; and the relationship of TT&C security to the much broader issue of total satellite systems security, including other NSEP features that might be requested by the government in the future.

3. Scope of Proposed Policy Statement

a. What is the intended scope of the proposed policy statement? While the briefers professed that it would not preclude the procurement of services by the government or government contractors from commercial satellite systems before the effective date of the policy, considerable further clarification is required.

- Will the proposed policy preclude the procurement of services from systems which were launched before the effective date if the government determines that secure TT&C is required for a particular application or program?

- Will the proposed policy apply to the procurement of all satellite services by the government and government contractors from systems which are launched after the effective date, or just for those applications or programs where secure TT&C is a stated requirement?

- As a practical matter, will government contractors be forced to procure satellite services only from government approved systems even though only a portion of their business is with the government?

b. Obviously, answers to these and related questions will greatly affect the results of the proposed policy from the government's perspective as well as the carriers response' to the policy if implemented. If broadly applied, the policy might cover a significant portion of commercial satellite business and the outcome might be quite different than if narrowly applied.

c. Certainly, the scope of policy application will influence satellite carrier technical and business decisions which in turn may affect their competitive position vis-a-vis other satellite and terrestrial carriers. It is possible that the policy might have anti-competitive consequences which would be of concern to the FCC. This important issue is addressed in more detail in the attached paper prepared by the Domestic Facilities Division of the Common Carrier Bureau.

d. Certainly, the scope of application will also impact the effectiveness of the policy from the government's perspective. If narrowly applied, some carriers may elect not to compete for government business. This could have several undesirable consequences including reduced competition, increased costs and government dependence on one or a few systems to provide essential communications. It is conceivable that the policy might produce a result counter to the government objectives of flexibility, redundancy and interoperability. Concentration of government traffic on one or two satellite systems might actually increase the possibility of disruption.

4. Countermeasures and the Threat

a. TT&C countermeasures appear to be extremely threat dependent both in terms of the nature of the threat and its duration. Some countermeasures are very effective against one or more types of threat and less effective or not effective at all against other types of threat. Not one technique discussed at the meeting was effective against all types of threat to TT&C. For example, continuous jamming can defeat crypto secure TT&C. And, of course, physical destruction of critical satellite components can render them inoperable regardless of measures taken to protect TT&C.

b. It appears that the carriers have already taken various measures to protect against unauthorized access to the TT&C of their satellite systems and have already established techniques and procedures for regaining control should TT&C malfunction or an unauthorized entity temporarily take control.

c. It appears that informed decisions by the government or carriers with respect to security of TT&C cannot be made until a more detailed analysis of threats and countermeasures is completed. This analysis should include not only the recommended technique but options presented at the NIAC meeting as well as techniques and procedures presently employed by the carriers.

5. Countermeasures and Cost

a. TT&C countermeasures are extremely cost variable, ranging from little or no additional cost to techniques requiring substantial additional expenditures by the carriers. Increased costs may be associated with design and construction as well as system operation of both satellites and ground stations. Also, weight/space considerations are particularly critical in satellite design as they directly affect longevity, capacity and other critical parameters.

b. As mentioned above, the carriers have already taken some measures to provide TT&C security and recovery capabilities in the event of malfunction or unauthorized access. The question is, how cost-effective are these measures compared with other possibilities and the technique recommended by the government. Cost considerations affect business decisions which in turn have competitive marketplace implications. The briefers presented virtually no information or analysis of any of these cost issues.

c. Again, it appears that an informed decision cannot be made on this matter until a more detailed analysis is completed of various countermeasures, including their costs.

6. Relationship of TT&C To Other Security Considerations

a. How do decisions regarding TT&C security relate to other commercial satellite system security requirements? This is another significant unanswered question which surfaced at the NIAC meeting.

b. TT&C Security addresses only one type of threat to just one component of a total satellite system. TT&C countermeasures are designed principally to deny satellite access by unauthorized entities or prevent unauthorized entities from denying control to the system owner/operators. It does not address jamming of control circuits, physical destruction or damage of vital satellite components, security of ground stations and communications links, hardening, interoperability, and other security concerns.

c. It appears that the present government structure for dealing with these issues is fragmented. The NTISSC charter is limited to certain aspects of the overall problem. Other forums, such as the NSTAC, are addressing equally if not more important satellite system security issues. Further, consideration of some of these issues has been deferred.

d. The carriers have limited resources to spend on total satellite system security and appear to be operating in a highly competitive environment with other satellite and terrestrial carriers. Accordingly, decisions regarding TT&C security (either by the government with respect to procurement policy or by the carriers themselves as they respond to the marketplace) should not be made out of context. Absent a "systems" approach which addresses the total problem and all viable solutions prior to the issuance of the government TT&C procurement policy, the carriers may make suboptimum business and investment decisions. They may take measures to guard against lower risk threats and protect less vulnerable system components at the expense of protecting more vulnerable system components against more likely threats. Large investments in TT&C countermeasures in response to the issuance of the proposed policy may preclude adequate investments in other aspects of system security at a later date. In other words, issuance of the procurement policy without further analysis might contribute to reduced rather than enhanced overall satellite system security. It is conceivable that a better overall outcome might result from the government's perspective if the policy statement is not issued. Further, as mentioned earlier, the proposed policy may have unintended anti-competitive consequences which would work counter to the governments overall objectives of providing reliable and secure satellite communications.

7. Reliability of Recommended Technique

a. At the NIAC meeting the carriers expressed concern about the reliability of the recommended technique. Irrespective of the other concerns expressed above, they are reluctant to proceed with the substantial investment required to incorporate the recommended technique into their satellite systems until its reliability is adequately demonstrated. In other words, they don't want to buy a "lock" when there is no assurance that the "key" will work. The recommended technique has apparently not been tested in a space environment. The briefers indicated it might be several years before tests are completed. This concern relates directly to the issuance and effective dates of the policy.

8. Conclusions and Recommendations

- Finalization and/or promulgation of the proposed procurement policy is premature absent extensive further study and analysis. Further, if adopted, the policy should state its purpose, scope,

and operation in the clearest possible terms in order to avoid the confusion and concerns generated by the draft.

- The commercial satellite industry already uses a variety of system design and operational techniques to provide a measure of TT&C security. They have suggested a number of other options. Full consideration should be given to all of these, including the government proposal, before the government policy statement is finalized and promulgated.

- Most important, decisions regarding government TT&C procurement policy should not be finalized absent a total satellite systems security analysis. This analysis should include consideration of all risks and threats including associated probabilities in relation to all viable countermeasures together with their effectiveness and costs.

- Accordingly, it is recommended that a government-industry mechanism be established to conduct this system analysis and submit findings and recommendations to appropriate government authorities.

Prepared By: Alan R. McKie, Deputy Managing Director, in coordination with Thomas P. Stanley, Deputy Chief Scientist -Operations, and James, R. Keegan, Chief, Domestic Facilities Division, Common Carrier Bureau.

Attachment

February 6, 1985
Domestic Facilities Division
Common Carrier Bureau

**Concerns Regarding and Proposed Revision
to National Policy on Application of
Communications Security to Civil Space Stations.**

The policy's overall approach is contractual: satellite carriers wishing to do business with the government directly must secure the systems over which they will carry government traffic, and those other companies which seek government contracts must send their communications over secured satellite systems. As a general proposition, the Commission does not interfere in the marketplace bargaining that goes on between a customer, such as the government, and service provider, such as a satellite carrier, in contracting for telecommunications services.

In this instance, however, anticompetitive problems may arise depending upon whether the policy, in its application to government contractor use of satellite systems, covers government contractor use of satellite services for all their business activities, or only use of such services to conduct that portion of their business which relates to performance of their government contracts. As currently drafted, the policy does not make clear whether the broader or narrower interpretation is intended, although its plain language makes it susceptible to the more far-reaching interpretation. Yet, such an attempt to control the telecommunications procurement choices of government contractors in their activities that are outside the scope of their business or contracts with the government, is problematic. While it may be an appropriate reflection and exercise of market power for the government to dictate, through what is in effect a government-wide procurement policy, the type of security its contractors must provide with respect to the telecommunications activities they undertake in connection with security related government business or even government business generally, an effort to influence all government contractor telecommunications practices in areas unrelated to government contracts has the potential to distort the marketplace forces normally governing the availability and selection of satellite systems and services. The government would be using its power in a capacity far beyond that of an ordinary communications service customer. By affecting the use of satellite systems for the total volume of satellite traffic generated by all the companies that do business with the government, the policy would have an impact on the satellite industry far out of proportion to the government's direct market power in this area. While we estimate that the government uses less than 5% of the total capacity of satellites now in orbit, if the policy were extended to all government contractor use of such systems for any purposes, it would influence a much more substantial, if not major,

- 2 -

segment of commercial satellite business. This effect may conflict with the Commission's pro-competitive policies aimed at minimizing government interference in marketplace structure and practices. Furthermore, while the NTISSC has the authority to issue national policies applicable to and binding upon the departments and agencies of the government, their authority to similarly bind private entities through a government policy statement, especially as to their non-government contract related activities, is questionable. Would the obligations under the policy be imposed on the contracting government agencies, the satellite carriers and/or the other commercial entities contracting with the government? What would be the relationship between these various obligations, and by what authority and mechanism would they be enforced? These issues require clarification. The policy would, in any event, be less troublesome to the FCC in its potential to disrupt normal marketplace forces and relationships if its reach with respect to government contractors were clearly limited to their use of satellite systems for communications related to performance of their government contracts alone. (See Attachment A for some suggested alternative language.)

SUMMARY MINUTES

FEDERAL COMMUNICATIONS COMMISSION
NATIONAL INDUSTRY ADVISORY COMMITTEE
COMMON CARRIER COMMUNICATIONS SUBCOMMITTEE

Tuesday, January 29, 1985

AT&T Communications
Tenth Floor Conference Room
1120 - 20th Street, N. W.
Washington, D. C.

Chairman: John Boning
RCA Corporation

Public Notice of Meeting Appendix A
Attendance List Appendix B
Meeting Outline Appendix C
Draft of proposed National Policy on
Application of Communications Security to
Civil Space Systems Appendix D
Background Correspondence Appendix E
Optional Methods of Providing TT&C Security . . Appendix F

The Chairman, Mr. Boning, opened the meeting at 9:45 A. M. by thanking AT&T for the use of the excellent facility to accommodate this NIAC Common Carrier Communications Subcommittee meeting on the protection of telemetry, tracking and control (TT&C) for commercial and civil satellites. He mentioned the documents provided as handouts to all meeting attendees (included as Appendices C, D and E of these minutes).

Mr. Boning cited some examples of verbage in the policy that needed clarification, such as "civil satellites" and "mission data." These definitions were subsequently clarified in the briefing by the National Security Agency (NSA).

Mr. Boning provided a brief history of the National Security Telecommunications Advisory Committee (NSTAC) Communications Satellite Subcommittee (CSS) analysis wherein recommendations were made to protect the TT&C, to harden terrestrial facilities against Electro-Magnetic Pulse (EMP), to enhance physical security against terrorist attack, to provide a capability for interoperability, to provide for protection of traffic, and to enhance emergency planning and procedures.

Mr. Boning pointed out that if we can fully understand the total threat to the satellite system, we can determine the most practical solution to the problem. The total threat is not just the TT&C problem. On 15 January SRI provided a terrorist activities briefing by the FBI, FEMA, ERDA, Treasury, and CIA. These federal agencies defined threats that were very real and as significant as the TT&C threat. Based on the above briefing, terrorism should be considered as a new form of warfare perpetrated by three general categories of terrorists, as follows:

- o State supported terrorists
- o Internal terrorists
- o Crazies

The primary threat is from the state supported terrorists who physically exist in this country. They are organized, equipped, trained and capable. Many of them are identified and are tracked by government agencies. The FBI defined their usual targets, particularly in Central America, as transportation, power, communications, finance and political targets. Their modus operandi is never very clear. They are very clever, they use surprise to the maximum extent and they desire spectacular results toward interrupting the status quo of orderly government. They capitalize on fear.

Mr. Boning stated that the reason for the meeting today is to discuss TT&C of commercial satellites and the protection thereof. There are several options to provide protection; each option has its drawbacks and all are scenario dependent. Even though this particular meeting is on TT&C, the carrier must also address all of the threats. The satellite carriers must be very careful in protecting against these threats lest their costs escalate to the point that their business picture is so burdened by protection systems that they can no longer be competitive. In such an event the terrorists would have won without ever challenging the system.

Mr. McKie of the Federal Communications Commission (FCC) stated that the meeting was called to provide information for Mr. Edward J. Minkel, the FCC Managing Director, prior to his participation in an upcoming meeting of the National Telecommunications and Information Systems Security Committee (NTISSC).

Mr. Boning introduced Mr. Noell Matchett of NSA who initiated a classified briefing on the threat to commercial satellite TT&C.

In an unclassified portion of the briefing NSA agreed to provide a high quality algorithm that can be embedded in the TT&C package of the satellite by the satellite manufacturers. The overall system would be unclassified but the computer chips would be controlled. With the agreement of the carriers NSA will provide counsel, expertise, evaluation and endorsement of the TT&C incorporated into commercial system.

The system will contain characteristics for interoperability. Radiation hardening of the subsystem is being developed but hardening is not required.

Five years after the adoption of a national policy on TT&C government Requests for Proposals (RFP's) may include a specification for protected TT&C.

NSA concluded that TT&C incorporation makes good sense to the government. NSA counsel, advice and guidance is available and all potential protection techniques will be considered.

Following the NSA briefing the subject was opened for questions and general discussion.

Several questions were asked involving the definition of the term, "civil satellite." These were defined as applications type satellites that generate on board information. METSAT and LANDSAT are in the civil satellite category.

Another series of questions involved the term, "mission data." This was defined as the data from civil satellites that develop on board information. There is no mission data on commercial satellites. This point is very significant because several of the carriers had interpreted "mission data" as commercial satellite through-put. If they became responsible for the protection of that data they would face a severe financial burden.

Another question was, "Why is the threat limited to accessing the satellite rather than destroying the satellite by lasers or high powered signals?" One answer was that the satellite could be held for ransom.

A question was posed based on the SRI briefing wherein the FBI defined threats against terrestrial facilities. Since the carriers must address such threats as well as inter-operability, EMP protection, and command survivability, the question asked if anybody is looking at the total threat package and making a systems analysis and cost estimate of all the protection needed. The answer indicated that this is an NSTAC problem but that NSTAC has not yet addressed it.

Further, the stated government strategy included a presumption that the free market will allow carriers to recoup cost on a competitive basis and that there may even be some insurance savings. Both of these statements were disputed by several carriers. Another point introduced was that, based on a survey, commercial entities were not interested in traffic protection. Nevertheless, costs resulting from protection systems will be passed along to the public.

Carriers reiterated the related point that as protection requirements increase, so does the cost of service. In the meantime, terrestrial point-to-point traffic costs are going down. The Chairman stated the carriers do not dispute the fact that encryption of TT&C is a good protection against the threat described by NSA but that the FBI has drawn up just as realistic a threat scenario which may include the destruction of satellites and terrestrial communication systems for which encryption provides no protection. The carriers expressed concern about how all of their protection efforts will be paid for. One of the carriers proposed tax incentives to help offset some of the more significant costs.

The Chairman interrupted the discussion in the interest of time and requested that a TT&C engineer describe several options to providing protected TT&C.

Mr. Lewin, RCA Manager of Satellite Operations, provided four options, each involving a different scenario. One option is a continuous high powered uplink carrier (Ku band) that would effectively jam the TT&C receiver to preclude accessing the system with present state of the art hardware. A second option is to raise the command threshold level on the satellite once orbit is established. A third option exists to shape the beam of the TT&C antenna to minimize its coverage. A fourth option is to incorporate intrusion

detection to provide a very rapid indication that the satellite is being accessed by outside parties; this system is installed in some satellites now and presumes an override capability at the TT&C station. A more complete description of the options discussed by Mr. Lewin are contained in Appendix F.


A carrier questioned whether or not the grandfathered systems (within five years of a National Security Policy on TT&C) would be ignored in the future in favor of the newer protected systems. The answer from a Defense Communications Agency (DCA) spokesman was that an RFP can state that there is a requirement for protection. In other words, there is nothing to stop a government agency from specifying TT&C protection before the grandfather period ends.


The open discussion ended and the Chairman summarized proposed submission of conclusions to the NIAC Long Range Planning Committee and the FCC as follows:

- o All solutions offered for the protection of TT&C are scenario dependent.
- o There are many security problems other than TT&C, including destruction of the satellite and/or ground facilities, and EMP considerations.
- o Costs of total security will significantly affect the competitive position of satellite carriers.

An overall conclusion to be drawn from the meeting is that there is a critical need to take a systems approach to the protection of satellite systems and communications resources in general prior to establishing a national policy on such a narrow aspect as TT&C of satellite communications. The terrorist threat is real and can be anticipated when it is politically expedient for the terrorists to attack.

The meeting was adjourned at 12:02 P. M..


Herbert J. Neumann
Executive Secretary, NIAC


John Boning
Chairman, Common Carrier
Communications Subcommittee



PUBLIC NOTICE

FEDERAL COMMUNICATIONS COMMISSION
1919 M STREET N.W.
WASHINGTON, D.C. 20554

1795

News media information 202/254-7674.

Recorded listing of releases and texts 202/632-0002.

FCC 85-1

35452

January 8, 1985

NATIONAL INDUSTRY ADVISORY COMMITTEE
COMMON CARRIER COMMUNICATIONS SUBCOMMITTEE

NOTICE OF MEETING

Pursuant to the provisions of Public Law 92-463, notice is hereby given of a closed meeting of the Common Carrier Communications Subcommittee of the National Industry Advisory Committee (NIAC) to be held Tuesday, January 29, 1985. This meeting is closed to the public under authority of Section 10(d) of the Federal Advisory Committee Act (P. L. 92-463, as amended). The Subcommittee will meet at 9:30 A. M. at AT&T Communications, 1120 - 20th Street, N. W., Washington, D. C. 20036, North Tower.

PURPOSE: Classified briefing concerning satellite communications matters.

AGENDA : As follows:

1. Opening remarks by Chairman.
2. Briefing and discussion.
3. Adjournment.

For more information about the meeting the NIAC Executive Secretary in the FCC Emergency Communications Division may be contacted at (202) 634-1549.

Action by the Commission January 4, 1985. Commissioners Fowler (Chairman), Quello, Dawson, Rivera and Patrick.

- FCC -

APPENDIX B

Page 1

Attendance List

NIAC Common Carrier Communications Subcommittee

January 29, 1985

Chairman

John Boning

RCA Consultant

NIAC Members

William Jack
 Charles Meizner
 James Orefice
 Coleman Guthrie
 George Tellmann, Jr.
 Jeff Kushan
 Lowell Thomas
 Angelo Nicosia
 Marianne Swindler
 Michael Shaw
 John Dunlop

AT&T Communications
 AT&T Communications
 AT&T Communications
 COMSAT General
 COMSAT
 GTE Sprint
 GTE
 ITT
 ITT
 MCI
 TRT

Other Industry

Stuart Meister
 Robert Yamazaki
 Robert Bradshaw
 Troy Ellington
 G. Jay Nelson
 Richard Heitman
 Jerold Jacaruso
 Al Prekeris
 Jacob Lewin
 Charles Somerville
 Donald Jansky

AMSAT
 COMSAT
 GTE
 GTE
 GTE Sprint
 ITT
 ITT
 ITT
 RCA Americom
 TRT
 TRT Consultant

Federal Government

Karl Brimmer
 Fred Goldsmith
 James Keegan
 Kevin Kelley
 Michael Marcus
 Alan McKie
 Herbert Neumann
 Jack Richards
 Raymond Seddon
 Anne Siegel
 Thomas Stanley

FCC
 FCC
 FCC
 FCC
 FCC
 FCC
 FCC
 FCC
 FCC
 FCC
 FCC

APPENDIX B

Page 2

Attendance List (Continued)

NIAC Common Carrier Communications Subcommittee

January 29, 1985

Federal Government (Continued)

Capt. David Brown	NCS
J. Randolph MacPherson	NCS
Benham Morriss	NCS
George Silberman	NCS
Milton Weiner	NCS

Arthur Altenburg	NTIA
------------------	------

STAT

APPENDIX C

**National Industry Advisory Committee
Common Carrier Communications Subcommittee**

Meeting Outline
January 29, 1985

Background and Objective:

- o The Government is formulating a national policy regarding the procurement of commercial satellite systems and services by Federal agencies and government contractors. This policy will address government requirements for communications security with respect to both message traffic and telemetry, tracking and control (TT&C).
- o The NIAC Common Carrier Communications Subcommittee has been convened by the FCC to provide a forum for the presentation and discussion of the potential threat to TT&C of commercial satellite systems, and the various measures which might be employed by the owners and operators of these systems in order to provide protection against this threat when required by the government. (The meeting will not address security of satellite message traffic.)
- o The government seeks information on the full range of options available, the merits and demerits of each, their costs, and any other information which may be useful in finalizing the proposed national procurement policy.
- o Additional government-industry meetings and discussions may be required to conclude technical evaluations of options identified at the meeting.

Order of Discussion:

1. Threat Briefing
2. One Proposed Solution to the Threat
3. Clarification of Draft Policy Statement
4. Identification and Discussion of Other Options to Counter the Threat
5. Summation

**NATIONAL POLICY
ON
APPLICATION OF COMMUNICATIONS SECURITY TO CIVIL
(U.S. GOVERNMENT AND COMMERCIAL) SPACE SYSTEMS**

SECTION I - POLICY

1. Government classified and Government or Government contractor national security-related information transmitted over satellite circuits shall be protected by approved techniques from exploitation by unauthorized intercept.
2. Government or Government contractor use of U.S. civil and commercial satellites launched five years from the date of this policy shall be limited to space systems using approved techniques necessary to protect the essential elements of telemetry, tracking and control (TT&C) and mission data.

SECTION II- EXCEPTIONS

3. Exceptions to this policy may be granted by the NTISSC in consultation with Federal departments and agencies as well as the private sector.

SECTION III - DEFINITIONS

4. Space systems consist of the spacecraft or satellite, command ground station, data acquisition stations, telecommunications, TT&C, and mission data functions.
5. Mission data is transmitted by the spacecraft to accomplish its operating objectives. Protected essential elements are those functions of TT&C which would deny unauthorized control of the space system.

SECTION IV - HEADS OF DEPARTMENTS

6. The Director, National Security Agency, in coordination with other departments or agencies as appropriate, shall assess space systems telecommunications, TT&C, and mission data functions to determine their vulnerability to unauthorized use and provide approved protection techniques and guidance.
7. Nothing in this policy shall relieve the heads of Federal departments and agencies of their authority and responsibility for executing other measures to assure the adequate protection of their telecommunications.



GTE Service Corporation

1120 Connecticut Avenue N.W.
Washington, D.C. 20036
(202) 463-5200

November 27, 1984

MEMORANDUM

**TO: Members, Long Range Planning Committee,
National Industry Advisory Committee**

**SUBJECT: National Policy on Applications of Communications
Security to Civil (U.S. Government and Commercial)
Space Systems**

The NIAC Long Range Planning Committee has been asked by the FCC to comment on a draft "National Policy on Applications of Communications Security to Civil (U.S. Government and Commercial) Space Systems."

The cover letter and draft policy requesting our assistance from Ed Minkel of the FCC is attached. An answer from the LRPC is expected before the Holidays.

Please provide your comments to me at 1120 Connecticut Avenue, N.W., Suite 900, by December 6, 1984. We will consolidate your comments and coordinate with each of you before an answer is provided to the FCC.

Since Commissioner Dawson and Ed Minkel are anxious to receive our comments, I would prefer not to convene a formal meeting of the LRPC, but stand ready to do so if necessary.

Thank you for your cooperation.

Sincerely,

A handwritten signature in cursive script that reads "C. J. McLean".

C. J. McLean
Vice President
Government Communications

CJM:mhf

Attachment

cc: Chairman Mark Fowler
Commissioner Mimi Weyforth Dawson

Honorable David Markey
Lt. Gen. Winston Powers

FEDERAL COMMUNICATIONS COMMISSION

WASHINGTON, D.C. 20534

November 21, 1984

IN REPLY REFER TO:

Cyrus J. McLean
Vice President - Government Communications
GTE Service Corporation
Stamford Forum, Stamford Conn. 06904

Dear Mr. McLean:

I am writing to you in your capacity as Chairman of the Long Range Planning Committee of the Commission's National Industry Advisory Committee. National Security Decision Directive 145 (NSDD 145), "National Policy on Telecommunications and Automated Information Systems Security," signed by the President on September 17, 1984, establishes initial objectives, policies, and an organizational structure for national activities aimed at safeguarding from hostile exploitation systems which process or communicate sensitive information. That Directive established, in place of the former National Communications Security Committee (NCSC), the National Telecommunications and Information Systems Security Committee (NTISSC), a working level interagency group operating under the direction of a senior level steering group, to consider technical matters and develop operating policies as necessary to implement the provisions of NSDD 145. The Commission participates in the NTISSC as an observer. As part of its effort, the NTISSC has prepared a draft "National Policy on Application of Communications Security to Civil (U.S. Government and Commercial) Space Systems." That policy, a copy of which is attached, would limit government and government contractor use of space systems to those which use "approved techniques" to protect the telemetry, tracking and control elements that are essential to control of the space system.

Because of the Commission's regulatory role in licensing domestic communications satellites, we have a responsibility to assess the impact of the NTISSC satellite security policy on the commercial satellite industry. One of NIAC's roles has been to advise the Commission on NSEP matters, and once again we look to your group for assistance. We request that you review the draft National Policy and provide the Commission with informal comments reflecting the consensus of your committee members by the end of the year. NIAC's evaluation of this important facet of the government's National Security and Emergency Preparedness efforts will enable the Commission to most effectively fulfill its regulatory responsibilities. Because the policy is in draft form, we ask that its circulation be limited to your committee members.

NIAC's work on NSEP issues have been of great value to the Commission in the past, and on behalf of the Commission I thank you for your

- 2 -

efforts in this vital area. We look forward to receiving your comments and to our continued cooperation.

Sincerely,

Edward J. Minkel
Edward J. Minkel
Managing Director

Enclosure

cc: Chairman Mark Fowler
Commissioner Mimi Weyforth Dawson
Honorable David Markey
Lt. Gen. Winston Powers

*John - Hope you have the
time to give this the attention
it deserves. Look forward to
seeing your response.*

Mimi

**NATIONAL POLICY
ON
APPLICATION OF COMMUNICATIONS SECURITY TO CIVIL
(U.S. GOVERNMENT AND COMMERCIAL) SPACE SYSTEMS**

SECTION I - POLICY

1. Government classified and Government or Government contractor national security-related information transmitted over satellite circuits shall be protected by approved techniques from exploitation by unauthorized intercept.
2. Government or Government contractor use of U.S. civil and commercial satellites launched five years from the date of this policy shall be limited to space systems using approved techniques necessary to protect the essential elements of telemetry, tracking and control (TT&C) and mission data.

SECTION II- EXCEPTIONS

3. Exceptions to this policy may be granted by the NTISSC in consultation with Federal departments and agencies as well as the private sector.

SECTION III - DEFINITIONS

4. Space systems consist of the spacecraft or satellite, command ground station, data acquisition stations, telecommunications, TT&C, and mission data functions.
5. Mission data is transmitted by the spacecraft to accomplish its operating objectives. Protected essential elements are those functions of TT&C which would deny unauthorized control of the space system.

SECTION IV - HEADS OF DEPARTMENTS

6. The Director, National Security Agency, in coordination with other departments or agencies as appropriate, shall assess space systems telecommunications, TT&C, and mission data functions to determine their vulnerability to unauthorized use and provide approved protection techniques and guidance.
7. Nothing in this policy shall relieve the heads of Federal departments and agencies of their authority and responsibility for executing other measures to assure the adequate protection of their telecommunications.



GTE Service Corporation

1120 Connecticut Avenue N.W.
Washington, D.C. 20036
(202) 463-5200

December 19, 1984

Mr. Edward J. Minkel
Managing Director
Federal Communications Commission
1919 M Street, N.W.
Room 852
Washington, D.C. 20554

Dear Mr. Minkel:

This responds to your letter of 21 November 1984, in which you ask for the National Industry Advisory Committee (NIAC) to comment on the draft executive branch policy on the "Application of Communication Security to Civil (U.S. Government and Commercial) Space Systems." I have asked the members of the NIAC Long Range Planning Committee for their thoughts on this matter.

Enclosed are the comments from a number of the members. As you can see the draft policy has raised a number of questions and concerns. Some of the areas in which there is uncertainty include:

- Ambiguity over what is intended by the policy;
- Appreciation for the nature of the threat;
- Clarification over the type of technique which may be used to protect commercial communications satellites.

As should be apparent, the NIAC membership is not now in a position to endorse this proposed policy. Many of the carriers' concerns could be alleviated if they receive information which would clarify the points raised. We recommend that this matter be referred to the Common Carrier Subcommittee for a

A part of GTE Corporation

classified briefing during January. The Common Carrier Subcommittee would then be in a position to make recommendations to the FCC.

Thank you for the chance to comment on this policy.

Sincerely,



C. G. McLean
Chairman, Long Range Planning Committee
National Industry Advisory Committee

CJM:dmp

Enclosures

cc:

Chairman Mark Fowler, FCC
Commissioner Mimi Weyforth Dawson, FCC
Honorable David Markey, NTIA
Lt. Gen. Winston Powers, NCS
Hubert J. Neumann, FCC

Long Range Planning Committee Members:

Robert F. Allnut, COMSAT Corp.
John Boning, RCA American Communications, Inc.
Eugene S. Cowen, American Broadcasting Company
Mark E. Crosby, Special Industrial Radio Service Association, Inc.
Charles Dorian, The American Radio Relay League, Inc.
Wallace Dunlap, Westinghouse Broadcasting Company
John Dunlop, TRT Telecommunications Corporation
Charles R. Dunn, Commercial Radio & Electronics
Eugene Eidenberg, MCI Telecommunications Corporation
Edward O. Fritts, National Association of Broadcasters
Joseph J. Gancie, ITT World Communications, Inc.
Arthur A. Garman, Western Union Telegraph Company
Robert E. Gradle, AT&T Technology Systems
Wayne Green, Wayne Green Enterprises, Inc.
Jerry M. Haleva, California Legislature
Robert D. Hynes, Jr., National Broadcasting Company, Inc.
Robert W. Kinzie, COMSAT General Corporation
Marvin W. Konow, Bell Communications Research, Inc.
E. J. Kushan, GTE Sprint Communications Corporation
C. Travis Marshall, Motorola, Inc.
Henry W. Meetze, Railing Corporation
Ron Nessen, Mutual Broadcasting System, Inc.
Richard O. Newman, Public Service Company of Oklahoma
Morgan E. O'Brien, Lukas, O'Brien and Raiser
Samuel F. Shawhan, GTE Corporation
Hillyer S. Smith, Jr., Aeronautical Radio, Inc.
Robert H. Snedaker, Jr., United Telephone System, Inc.
John B. Summers, National Association of Broadcasters
Roy M. Teel, Jr., MSI Communications, Inc.
Donald D. Wear, Jr., CBS, Inc.

Inter-Office Memo



To: Lowell Thomas
From: Leslie A. Taylor, GTE Spacenet Corporation
Date: December 19, 1984
Subject: Proposed National Policy on Government or Government Contractor Use of U.S. Civil and Commercial Satellites

GTE Spacenet Corporation

The following are the concerns of GTE Spacenet relative to the NSTAC proposal on the Draft National Policy on Application of Communications Security to Civil (U.S. Government) and Commercial Space Systems.

1. The purpose(s) of the proposed policy needs clarification.
 - (a) is the purpose to provide protection to government classified traffic carried over commercial systems?
 - (b) is the purpose to prevent access by unauthorized persons to the facilities of commercial space system operators?
 - (c) is the purpose to ensure that protection is available over commercial systems in the event the government needs to utilize such systems in a national emergency?
 - (d) is the purpose all of the above?
2. What is the definition of "approved techniques?" Will commercially available encryption equipment be adequate, or will NSA equipment or NSA approved equipment be required? The costs and feasibility of various requirements could vary greatly.
3. The grandfather clause may not adequately protect companies such as GTE which is now deploying its satellite system. The thrust of the policy appears to indicate a strong preference for protection and this is likely to appear in RFPs, thereby excluding GTE from such government business. There are certain other companies which would be in a strong position with such a policy in place.

Proposed National Policy
December 19, 1984
Page two

4. The cost/benefit trade-off for the private satellite operator is really unknown, particularly because of the uncertainty as to what equipment would be required, and if any government classified business would ultimately be obtained, even if systems are retrofitted.
5. Are there comparable requirements imposed or proposed for terrestrial communications systems?
6. Under Definitions, what does "data acquisition stations" mean? Does it mean earth stations, transmit/receive?

Conclusion: While GTE Spacenet can understand the government's desire to have commercial operators bear the expense of installing protection devices on space systems, the draft policy is so vague that it provides insufficient guidance as to how an operator can quantify the costs of so doing, the benefits of so doing, or even if the installation of protection devices would satisfy the government's requirements.

Please let us know if we can be of additional assistance in this matter.

Leslie A. Taylor

Leslie A. Taylor
Director, Regulatory Affairs

1259P



November 29, 1984

Mr. C.J. McLean
Vice President - Government Communications
GTE Service Corporation
1120 Connecticut Avenue, N.W.
Suite 900
Washington, D.C. 20036

Dear John,

This is in response to your November 27, 1984 memorandum concerning the proposed "National Policy on Applications of Communications Security to Civil (U.S. Government and Commercial) Space Systems".

As you know, neither Bell Communications Research nor the Bell Operating Companies that we support are in any way involved in satellite communications systems. For that reason, I do not feel it would be appropriate for us to comment on the proposal.

I look forward to working with you on future issues where our input could be helpful.

Sincerely,

A handwritten signature in dark ink, appearing to read "M.W. Konow".

M.W. Konow
Assistant Vice President
National Security and Emergency Preparedness

MWK-plb



A. A. GARMAN
VICE PRESIDENT AND GENERAL MANAGER

December 4, 1984

Mr. C.J. McLean
Vice President
GTE Service Corporation
1120 Connecticut Avenue N.W.
Washington D.C. 20036

Dear John:

I have reviewed the draft National Policy on Application of Communications Security to Civil (U.S. Government and Commercial) Space Systems attached to your letter dated November 27, 1984.

The wording of Section I - Policy, and Section III - Definitions, is unclear and is likely to lead to confusion. Section I, Paragraph 2 introduces a new element, "mission data". Section III states that "mission data is transmitted by the spacecraft". Since Section III, Paragraph 4 differentiates between spacecraft and satellites, I assume spacecraft are shuttles or space probes or the like. Since we service suppliers only deal in satellites I do not understand what satellite-originated information is being referred to which would need to be protected. This should be clarified.

Section I - Policy, Paragraph 1 deals with information transmitted over satellite circuits and this is certainly the prerogative of the Government user. This can be implemented at any time and is basically a function of cost.

Section I, Paragraph 2 deals with protection of the TT&C which is understandable. It is not clear that such a mandate is in the best interest of the country (all suppliers of TT&C must be protected for all launches after five years from the date of the policy). The obvious individual advantages of satellite protection must be weighed against the technical problems posed in the face of solving the satellite interoperability question being addressed by NSTAC. Clearly, this issue should be thoroughly discussed with NSTAC.

If I may contribute further, please do not hesitate to call me.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Don Newkirk', with a large, stylized flourish below it.

for
Arthur A. Garman

RCA American Communications Inc | 400 College Road East | Princeton, NJ 08540 | Tel (609) 734-4380
FAX (609) 734-4380 | Telex 244010

Mr. C. J. McLean
Vice President GTE
1120 Connecticut Ave., N.W.
Washington, DC 20036

RCA

November 29, 1984

Dear John:

Government Services

Reference is made to your memo dated 27 November 1984, Subject: National Policy on Applications of Communications Security to Civil (U.S. Government and Commercial) Space Systems.

The enclosed paper lists the problems and questions generated by each paragraph of the proposed national policy.

We find the policy paper severely lacking in definition and intent. I recommend that we convene a closed session of the Common Carrier Subcommittee or an informal gathering of the same group with representatives of NTIA to clarify what the government wants and what can be done for the government with and without support funding.

Regards,


John Boning
RCA Member NIAC

JB:glt
Enclosure

COMMENTS ON PROPOSED NATIONAL POLICY

The following comments on the draft National Policy are provided for each paragraph contained therein.

Section I - Policy Paragraph 1

"Government classified and Government or Government contractor national security - related information transmitted over satellite circuits shall be protected by approved techniques from exploitation by unauthorized intercept."

Comment

To the best of our knowledge and belief, this policy has been in effect for an extended period. The Government determines the classification of information and is responsible for its protection. For the purposes of transmitting this information if it is classified, the government encrypts the data and provides an encrypted bit stream to the carrier who delivers the encrypted data to the premises of the receiving user. The receiving user decrypts the bit stream. Encryption equipment is not commonly provided to the carrier. The government is responsible for using government approved encryption techniques.

Section I - Policy Paragraph 2

"The government or government contractors use of U.S. civil and commercial satellites launched five years from the date of this policy should be limited to space systems using approved techniques necessary to protect the essential elements of telemetry tracking and control (TT&C) and mission data."

Comment

This paragraph is not entirely clear in the following areas.

- a. What is meant by a civil satellite and how does it differ from a commercial satellite?
- b. What is the date of the policy - when does the 5 year time period start? Depending on when an "approved" system will be available, the five years may not be realistic.
- c. It is assumed from reviewing paragraph 6 below that the approving authority of techniques used in protection of TT&C is NSA. This should be stated. Also, a departmental contact point needs to be established. If any other agencies or departments are involved in the approval, they should be listed to provide a definitive contact(s) for carriers trying to determine their appropriate action and when it is satisfactorily completed.

- d. The term "mission data" may be interpreted several ways. Since the mission of the satellite is to relay data between terrestrial points, it is assumed that this policy is directed toward specific circuits that need to be protected. Is it the intent of this policy to have the carrier responsible for encrypting the circuits to be protected?

Section II - Exceptions Paragraph 3

"Exceptions to this policy may be granted by the NTISSC in consultation with Federal departments and agencies as well as the private sector."

Comment

Since RCA American Communications, Inc. has not been provided with a copy of NSDD 145, it is not clear as to who is the approving authority for exceptions.

Section III - Definitions Paragraph 4

"Space systems consist of spacecraft or satellites, command ground station, data acquisition stations, telecommunications, TT&C, and mission data functions."

Comment

See comment in paragraph (d) under Policy Paragraph 2. "Mission data functions" is ambiguous.

Section III - Definitions Paragraph 5

"Mission data is transmitted by the spacecraft to accomplish its operating objectives. Protected essential elements are those function of TT&C which would deny unauthorized control of the space system."

See above comments on mission data. This definition does not clearly define what is meant by the term mission data. The spacecraft does not initiate transmission.

Section IV - Heads of Department Paragraph 6

"The Director, National Security Agency, in coordination with other departments or agencies as appropriate, shall assess space systems telecommunications, TT&C, and mission data functions to determine their vulnerability to unauthorized use and provide approved protection techniques and guidance."

This activity, to be successful, should have the full participation of each carrier concerned since each carrier resources have different characteristics.

Section IV - Heads of Departments Paragraph 7

"Nothing in this policy shall relieve the heads of Federal departments and agencies of their responsibility and authority for executing other measures to assure the adequate protection of their telecommunications."

No Comment

General Comments and Questions

- a. Encrypted TT&C links are vulnerable to jamming - extended jamming can cause a loss of control of the satellite.
- b. Does this policy directive provide for monies necessary for TT&C encryption, software modification, security measures and physical TT&C site security, and training?
- c. Does this policy directive contemplate placing the responsibility for broad band traffic encryption on the carrier?

- d. Can paragraph 6 be interpreted to mean that NSA will pay for expenses associated with encryption?
- e. If the carriers are to pay for the equipment associated with this policy, how would the government address the problem of competition with terrestrial systems who presumably handle traffic in the time proven manner and do not have the financial burden of encryption?
- f. Does the proposed policy contemplate modifying all satellites capable of handling government traffic whether or not they are used for that purpose (i.e. an exclusively all video distribution satellite).
- g. Is the government aware that a hi-powered uplink carrier that saturates the TT&C receiver, can provide more protection against a conus originated signal than an encrypted uplink?
- h. There are more credible threats than acquiring TT&C such as burning out the front ends on the receivers or burning out the earth sensors.
- i. I suggest that this policy be discussed among the carriers and the drafters of this policy paper and NSDD 145. It may be more easily handled with the NIAC Commission Carrier Committee rather than the entire Long Range Planning Committee. Until some of the above questions are answered, RCA cannot provide a position on this ambiguous document.



A Subsidiary of the
Association of
American Railroads

Henry W. Meetze
President

November 30, 1984

Mr. C. J. McLean
Vice President
Government Communications
GTE Service Corporation
1120 Connecticut Ave., NW
Washington, DC 20036

Dear Mr. McLean:

Reference, your memo of November 27, 1984, regarding National Policy on Applications of Communications Security to Civil (US Government and Commercial) Space Systems. I raise a concern regarding execution of that policy by the National Security Agency, but not with the policy itself which is quite broad. Specifically, I believe the commercial sector should be assured that the "approved protection techniques" provided by NSA will neither inhibit the commercial use of satellite communications nor the exploitation of that technology. Thank you for the opportunity to comment on the draft policy.

Sincerely,

A handwritten signature in dark ink, appearing to read "H. W. Meetze", with a long horizontal flourish extending to the right.

RAILINC CORPORATION • 1920 L Street, N.W. • Washington, D.C. 20036
202/835-9400



COMMUNICATIONS
SATELLITE
CORPORATION

Robert F. Allnutt
Vice President
Government Affairs

December 13, 1984

Mr. C. J. McLean
Vice President
Government Communications
GTE Service Corporation
1120 Connecticut Ave., NW
Washington, DC 20036

Dear Mr. McLean:

This responds to your memorandum of November 27, 1984, to the Members of the Long Range Planning Committee of NIAC. On behalf of COMSAT, I want to thank you for the opportunity to provide comments on what we deem as an important evolving national policy.

Last year, the National Satellite Telecommunications Advisory Commission (NSTAC) recommended that operators of commercial communications satellites should (a) in the short term, provide some method of command link protection; and (b) in the longer term develop, with the government, a command link encryption standard. NSTAC also reviewed telemetry encryption and decided that this was not required to protect satellites against unauthorized command access.

We agree with the NSTAC conclusions.

With regard to the five-year grace period proposed by the policy, we feel that this is a reasonable period and would urge its retention in any policy that is finally adopted. We would suggest that a useful next step should be working level meetings between representatives of the government and the industry--both manufacturers and satellite owners--to discuss the means of implementing the policy in detail. In this regard, we believe that the government should set standards for command link protection rather than issuing detailed specifications for encryption equipment or other means of protection.

Sincerely,



Robert F. Allnutt

950 L'Enfant Plaza SW
Washington, DC 20024
Telephone: 202-863-6313
Telex: 892664

COMMITTEE MEMBERS

ASSEMBLYMAN MIKE RIOS
VICE CHAIRMAN
SENATOR ALFRED ALQUIST
SENATOR WILLIE L. BROWN JR.
SENATOR WILLIAM A. CRAVER
SENATOR ED DAVIS
ASSEMBLYMAN PATRICK NOLAN
ASSEMBLYMAN LOUIS J. PAPAN
SENATOR ROBERT PRESLEY
SENATOR DAVID ROBERTS
ASSEMBLYMAN LARRY STYLING
ASSEMBLYMAN GALLY TANNER

ADVISORY BOARD MEMBERS

CHIEF RICHARD ANDERSON
QUINCY VOLUNTEER FIRE DEPARTMENT
CHIEF RICHARD BARROWS
OFFICE OF EMERGENCY SERVICES
FIRE AND RESCUE DIVISION
RONALD W. BODARDUS, P.E.
STATE FIRE MARSHALL
CHIEF CLYDE A. BRADSON, JR.
LOS ANGELES COUNTY FORESTER
AND FIRE WARDEN
SHERIFF JOHN W. CARPENTER
SANTA BARBARA COUNTY
MR. JAMES W. COLEOUNOON
COMMUNICATIONS DESIGNER RETIRED
CHIEF KENNETH CONDON
SAN FRANCISCO CITY FIRE DEPARTMENT
MR. GLEN CRAM
DIRECTOR
DIVISION OF LAW ENFORCEMENT
CALIFORNIA DEPARTMENT OF JUSTICE
MR. THOMAS G. DANDY
EXECUTIVE DIRECTOR
BERKELEY/MARIN COUNTY RED CROSS
MR. JAMES L. EASTON
ASSISTANT DEPUTY
LOS ANGELES COUNTY FLOOD CONTROL DISTRICT
CHIEF DARYL GATES
LOS ANGELES CITY POLICE DEPARTMENT
MR. R. C. HELMS
LOS ANGELES POLICE PROTECTIVE LEAGUE
MR. DALLAS JONES
VICE PRESIDENT
FEDERATED FIRE FIGHTERS OF CALIFORNIA
MR. BILL BEDROVICH
DIRECTOR
OFFICE OF EMERGENCY SERVICES
MR. WILLIAM J. PATTERSON
FEDERAL EMERGENCY MANAGEMENT AGENCY
MR. JOHN POWELL
PRESIDENT, NORTHERN APCO
U.C. BERKELEY
MR. CAROLINE PRATT
PRESIDENT
CALIFORNIA EMERGENCY SERVICES ASSOCIATION
MR. WILLIAM RIGGS
CALIFORNIA AMBULANCE ASSOCIATION
MAJOR GENERAL WILLARD A. SHANK
COMMANDER
CALIFORNIA NATIONAL GUARD
COMMISSIONER JAMES E. SMITH
CALIFORNIA HIGHWAY PATROL

California Legislature



Joint Committee

on

Fire, Police, Emergency and Disaster Services

SENATOR WILLIAM CAMPBELL
CHAIRMAN

December 5, 1984

Mr. C.J. McLean
Vice President, Government
Communications
GTE Service Corporation
1120 Connecticut Avenue, N.W.
Washington, D.C. 20036

Dear Mr. McLean:

Upon reviewing the draft "National Policy on Telecommunications and Automated Information Systems Security," I concur with the need to safeguard from hostile exploitation those telecommunications systems that process sensitive information. It appears that the identified objectives and policies for developing the necessary safeguard measures could be successfully implemented given the proposed organizational structure.

My only concern is in regard to the role and input of the Federal Communications Commission in this project. Since the FCC is responsible for licensing and regulating domestic telecommunications systems, I firmly believe that those individuals involved in the decision making process should consult with the Commission. I am confident that a cooperative arrangement can be established to bring that about.

ROOM 300
1100 J STREET
SACRAMENTO CA 95814
TELEPHONE (916) 445 1551

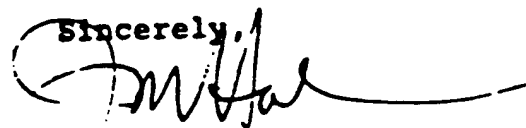
JERRY M. MALEYA
CHIEF OF STAFF

COMMITTEE STAFF
R. BLANK SPRINGER
PRINCIPAL CONSULTANT
ROBERT B. GORBER II
ASSOCIATE CONSULTANT
BLU. MARSHOTO
COMMITTEE SECRETARY

Mr. C.J. McLean
December 5, 1984
Page two

Thank you for allowing me the opportunity to comment on this draft policy. If I can be of any assistance, please contact me at your convenience.

Sincerely,

A handwritten signature in dark ink, appearing to read "J. Haleva", with a long horizontal flourish extending to the right.

JERRY M. HALEVA

JMH:slf

MEMO TO THE COMMON CARRIER SUB COMMITTEE

Re: "The National Policy On Application of Communications Security to Civil Space Systems"

The Common Carrier Sub Committee has been asked to address the above national policy for adequacy and acceptability to the Common Carriers. A survey was conducted by the Long Range Planning Committee and the consensus was that the policy was ambiguous in several important areas. Some terms were not clear. The intent of the government as to how the services are to be provided is not clear. The threat is not well defined.

Section 1 of the Policy paragraph 2 indicates two needs:

- (1) Protection for classified government communications.
- (2) A protection of presumably unclassified but sensitive government contractor security related information.

Protection of the communication of classified government information in accordance with existing policy, is the responsibility of the originator of the transmission. This is usually done by providing the carrier with an encrypted bit stream that is transmitted to the receiving agent who in turn decrypts the signal. This represents no problem to the carriers and has been a standard operation for some years.

Protection of the unclassified data is less clear. Is the protection DES or KG equipment? Is the protection circuit by circuit or by bulk encryption. How is analog handled? The circuit by circuit protection is not a problem if the originator provides a protected bit stream to the carriers. However, if the

carrier is to provide bulk encryption as a service, this is a problem that warrants considerable discussion and definition.

Paragraph 2 of Section 1 defines a need to protect "the essential elements of Tracking Telemetry and Control (TT&C) and mission data." Definition is required on the word "protect" and the words "mission data." Is the protection system defined by the carrier at the government? If the government defines a system that places a financial burden on the carriers, does the government assume financial responsibility?

Much of the system definition problem is a lack of a clear threat analysis that defines the problem to be solved. NSDD 145 indicates the threat is the interception of classified or sensitive data by foreign nations, terrorist groups and criminal elements. If the problem is interception then there is not so much concern at TT&C.

Each of the above groups have different interests. The interception problem has been with us for many years and it is manageable. Procedures exist for government contractors to be reimbursed for their efforts to secure information. The terrorist problem is on the increase. Terrorists are becoming more sophisticated. There is some unanimity among knowledgeable people in the government that terrorists by design do not perform large coordinated efforts. Rather they perform spectacular operations with relatively few people to bring about political change by public opinion and feelings of insecurity. There are however enough of the more notorious terrorist groups in the United States to perform coordinated operations if they want

to. Power systems and communication system have been targets in Central America - primarily transmission towers, power stations and antennas.

It is no clear who is interest in TT&C. The following questions address the TT&C problem and tend to help carriers to understand the problem to be solved.

THREAT

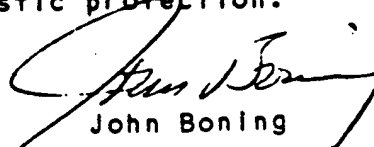
- (1) Who is the "enemy"?
- (2) Why does he want to access the satellites?
- (3) What does he want to do with the satellite?
- (4) Does he want temporary disruption, permanent disruption, destruction, or to steal it?
- (5) What technique will he use?
- (6) What are his assets to acquire access to the satellite?
- (7) How many satellites can he access at once and how frequently?
- (8) Is there a factual background that indicates that he will, in fact, make an attempt to access a satellite, or is there just a suspicion that he may possibly act against a satellite?
- (9) Why is accessing the satellite preferable to jamming it or destroying it?

TECHNOLOGY

- (1) Are there more than four options for the protection of the TT&C of the satellites?

- (a) D E S - Available now.
 - (b) NEW N S A algorythm - Available 6 - 18 months.
 - (c) Jamming the uplink - Available now.
 - (d) Inhibit system - Available 6 - 12 months.
- (2) How long will the D E S equipment be acceptable as a means of protection to N S A? 1 - 3 years, 3 - 6 years, over 6 years?
- (3) How long will the new N S A algorythm be acceptable to N S A as a means of protection? 1 - 5 years, 1 - 10 years, over 10 years?
- (4) Jamming the uplink appears to be a good means of prohibiting access to the satellite. Why is this more cost effective technique not acceptable against such an ill defined threat?
- (5) Is the "inhibit" system capability an acceptable amount of protection when coupled with a jamming capability?
- (6) Most carriers have in orbit spare satellites in event of the catastrophic loss of an operational satellite. Is this considered as protection?
- (7) What is the government intent - why?

There will be further demands on carriers to protect other portions of their systems. We need to look at the most cost effective means to provide realistic protection.


John Boning

APPENDIX F

February 8, 1985

RCA

Mr. Herbert Neuman
Executive Secretary, NIACC
Federal Communications Commission
Room BB #324
Washington, D.C. 20554

Dear Mr. Neuman,

As per your request, enclosed is the summary of my remarks at the National Industrial Advisory Committee Common Carrier Communications Sub-committee meeting on the protection of telemetry tracking and control (TT&C) for commercial satellites of 29 January 85.

Please feel free to call on me if I can be of any further assistance.

Best regards,



Jack Lewin, Mgr.
Mission Operations

JL:eb

cc: J. Boning

(secure commanding)

Commercial Communications Satellites are said to be vulnerable to unfriendly intrusion via the command system with the intruders ultimate aim of disruption of communications service, and for incapacitating the satellite for extensive periods or permanently. The preceding attacks are said to be particularly inopportune were they to occur during periods of urgent need, such as a world crisis or national emergency. It is during such periods that the Government would like to be able to count on the availability of commercial communications satellites to continue Government business carried thereon to a large extent and/or to supplement other Government owned communication capacity. Commercial communications satellites comprise an available resource of major proportions (approximately 20 satellites - 1985 and more than double that number currently authorized and expected to be launched by 1986).

It should be noted that the given objective of a "long term" or permanent denial of communications service ascribed to the unfriendly intruder can be attained via means other than spoofing the satellite command system, some of which might be attainable more effectively by certain types of unfriendly agents. For example, destruction of Earth Sensors via lasers, destruction of the communications or command receivers via high power klystrons (Giga Watts-pulsed) currently available or under development, placing noise generators near TT&C sites within side lobes of ground TT&C antennas effectively precluding telemetry reception, jamming either the communications or command receivers with high power carrier or physically destroying TT&C sites. Thus command system intrusion is an avenue of attack, singled out, perhaps out of context with the total range of interrelated possibilities.

Within the above context, the suggested countermeasure of commercial communications satellites command link encryptions without assessment and in isolation of other attack possibilities is perhaps premature. Limiting this discussion to command link intrusion, however, other counter measures intended to deny unfriendly access can be named, with potentially less costly consequences:

1. High Power Command Carrier - permanently on and beamed to the satellite. Given the typical FM satellite command receiver with limiting, unfriendly intrusion would be possible only by another carrier whose power levels were 2-4 dB higher. With existing dedicated, per satellite large aperture (9-14 meter) antennas at TT&C sites, this approach would effectively limit all but resource rich potential intruders.
2. Satellite Command Antenna Beam Shaping - The typical "omni" antennas providing broad coverage during transfer orbit or during spinning of the satellite is not considered here. Generally commanding via omni antennas requires significantly (10dB) more power than via the communications antenna. Additionally this antenna can be switched "off"

when on-orbit, and automatically reconnected should the satellite lose earth lock and begin to spin out of the communications antennas "footprint".

The potential intrusion threat is greater when command receivers are accessed via the high gain communications antenna with its expansive conus coverage and beyond footprint area. In contrast, on-orbit commanding needs can generally be satisfied by very limited "spot beams" or significantly narrowed footprint drastically decreasing the gain from offshore or transborder regions. This would require the intruder to use substantially greater resources to provide very large (30 meter +) antennas, to gain commanding access outside of the "footprint" area.

3. Raise The Command Receiver Threshold - commandable while on-station, necessitating higher power by the intruder.
4. Provide Intrusion Detection - via Telemetry. This capability currently exists in a number of satellites. This implies an override capability from the detecting TT&C sites.

The preceding are but a few ideas that come to mind. They can be used singly or in combination. Each is effective to a greater or lesser degree on the type of intruder threat postulated: i.e. it is scenario dependent.

The same can be said of command link encryption. The scenario of a hostile command jammer threat, for example, would, if allowed to persist long enough (hours to days), result in loss of communications or loss of the satellite even with encryption. In some cases jamming might, as is likely to be the case-by design, force the command system to revert to a "clear text" mode, allowing intrusion freely.

The common thread throughout the preceding discussion is commanding power. An intruder without the ability to keep out TT&C attempts to overcome or correct whatever upset might have been caused by him, will prove less effective. As discussed earlier, encryption can be defeated via jamming of the command link or the telemetry link. Thus the ultimate counter to a potential intruder is the ability to uplink more power than the intruder, short of receiver destruction. A continuous high power carrier will effectively keep all lower power intruders out and retain control of the satellite. Spread Spectrum may be the optimum approach to high power systems.

The preceding represent some ideas on the subject of satellite command link protection from hostile intruders whose objective is said to be the long periods (days to weeks) or permanently denial of a satellites communications capacity. It enumerates without discussion some other possible attack scenarios aimed at the same end. Clearly, a comprehensive "system" assessment as to the "Threat" and its countermeasures needs to be made before a determination as to the nature and scope of command protection is undertaken.